

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

UNITED STATES OF AMERICA

v.

OLALEKAN JACOB PONLE,
also known as "Mr. Woodbery,"
and "Mark Kain"

CASE NUMBER: 20 CR 318

UNDER SEAL

FILED

JUN 25 2020

CRIMINAL COMPLAINT

MAGISTRATE JUDGE

YOUNG B. KIM

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

Beginning no later than in or about January 2019 and continuing until at least September 2019, at Chicago, in the Northern District of Illinois, Eastern Division, and elsewhere, the defendant(s) violated:

*Code Section**Offense Description*Title 18, United States Code, Section
1349

Wire fraud conspiracy

This criminal complaint is based upon these facts:

☒ Continued on the attached sheet.

SADIQ.ALI.G95F98E79

2020.06.25 16:47:51 -05'00'

ALI SADIQ

Special Agent, Federal Bureau of Investigation
(FBI)

Pursuant to Fed. R. Crim. P. 4.1, this complaint is presented by reliable electronic means. The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: June 25, 2020City and state: Chicago, Illinois
YOUNG B. KIM, U.S. Magistrate Judge*Printed name and title*

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS

AFFIDAVIT

I, ALI SADIQ, being duly sworn, state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have been so employed since approximately September 2015. My current responsibilities include the investigation of violations of federal criminal law, including computer crimes, in violation of 18 U.S.C. § 1030 (the “Computer Fraud and Abuse Act”) and related frauds, including wire fraud.

2. This affidavit is submitted in support of a criminal complaint alleging that OLALEKAN JACOB PONLE, also known as “Mr. Woodbery,” and “Mark Kain,” has violated Title 18, United States Code, Section 1349. Because this affidavit is being submitted for the limited purpose of establishing probable cause in support of a criminal complaint charging PONLE with wire fraud conspiracy, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that the defendant committed the offense alleged in the complaint.

3. This affidavit is based on my personal knowledge, information provided to me by other law enforcement agents, statements of witnesses, my review of communications involving PONLE, and other documents and reports.

I. BACKGROUND INFORMATION

Business Email Compromise Schemes

4. In a typical business email compromise scheme (“BEC scheme”), a malicious actor compromises legitimate business email accounts through computer intrusion techniques or social engineering and uses those accounts to cause the unauthorized transfer of funds. Techniques for perpetrating these schemes include phishing, spear phishing, identity theft, email spoofing, and the use of malware.

Bitcoin

5. Bitcoin is a type of cryptocurrency, or virtual currency. Bitcoin is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Bitcoin transactions are recorded in the Bitcoin blockchain. The blockchain is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every bitcoin transaction.

6. People can send and receive cryptocurrencies online using many types of electronic devices, including laptop computers and smart phones. Even though the public addresses of those engaging in cryptocurrency transactions are recorded on a blockchain, the identities of the individuals or entities behind the public addresses are not recorded on these public ledgers. Bitcoin transactions are therefore sometimes described as “pseudonymous,” meaning that they are partially anonymous. And while it’s not completely anonymous, Bitcoin allows users to transfer funds more anonymously than would be possible through traditional banking and financial systems.

7. Blockchain analysis is the process of inspecting, identifying, clustering, modeling and visually representing transaction data on a blockchain. This process can be used to verify that transactions involving a wallet address occurred. It can also be used to obtain information about the individual or entity linked to a wallet address and thereby potentially identify that individual or entity.

8. Although cryptocurrencies such as bitcoin have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes such as money laundering. As of June 22, 2020, one bitcoin is worth approximately \$9,641.66, though the value of bitcoin is generally much more volatile than that of fiat currencies.

9. Bitcoin exchanges, such as Gemini Trust, are companies which allow individuals to purchase or sell cryptocurrencies in exchange for fiat currencies or other cryptocurrencies. Peer-to-peer cryptocurrency trading platforms, such as Localbitcoins.com and Paxful.com, facilitate over-the-counter trading of local currency for bitcoin.

II. FACTS SUPPORTING PROBABLE CAUSE

10. Beginning no later than January 2019 and continuing until at least September 2019, OLALEKAN JACOB PONLE conspired with others to engage in BEC schemes to defraud several United States-based companies. These schemes resulted in attempted and actual losses to victim companies in the tens of millions of dollars.

11. As described below, as part of the scheme, PONLE directed money mules in the United States to open bank accounts in the names of victim companies. Proceeds from BEC schemes, ranging from hundreds of thousands of dollars to millions of dollars, were then wired by unwitting employees to the bank accounts opened by PONLE's mules. PONLE then instructed the mules to convert the proceeds to Bitcoin and to send the proceeds of the BEC schemes to a bitcoin wallet that he owned and operated.

12. One of these BEC schemes involved a Chicago-based company (Victim Company A) that was defrauded out of \$2,300,000. A second Chicago-based company (Victim Company K) was defrauded into sending wire transfers totaling \$15,268,000.00. Preliminary blockchain analysis indicates that PONLE received at least 1,494.71506296 bitcoin related to these BEC schemes, valued at approximately \$6,599,499.98 at the time he received the proceeds.

A. PONLE Used the Alias "Mark Kain" To Correspond with Money Mules

12. As described in more detail below, money mules in the United States were approached by a person they knew as "Mark" or "Mark Kain." "Mark" later directed them to open bank accounts in the names of victim companies. Those accounts received proceeds from the BEC schemes, and at "Mark's" direction, the money mules converted proceeds to bitcoin and sent proceeds to "Mark".

13. According to one of those money mules, Individual B, "Mark Kain" contacted Individual B using telephone number (323) 985-4088 ("the 4088 phone number"). According to records obtained from Dingtone, a messaging and Voice over

Internet Protocol¹ application, subscribing customer records for the 4088 phone number included the cellular telephone number 27793837890 (“the 7890 phone number”), which based on law enforcement database searches, is owned by a South African service provider.

14. Based on my review of chat transcripts from online messaging applications between PONLE and Individual B and a second money mule, Individual A, “Mark” instructed Individual B and Individual A to send money to the bitcoin wallet 16AtGJbaxL2kmzx4mW5ocpT2ysTWxmacWn (“the 16AtGJ BTC Wallet”) on at least nine occasions. Records obtained from Bitpay, a processor of cryptocurrency transactions, indicated that between approximately September 18, 2015 and November 29, 2016, the 16AtGJ BTC wallet made five purchases associated with the Gmail account hustleandbustle@gmail[.]com (the “hustle Gmail account”).

15. Based on records obtained from Apple, an iCloud account (Subject Account 1) was subscribed to by Jacob Olalekan, listing the 7890 phone number, the hustle Gmail account, and a physical address in Johannesburg, South Africa.

16. Based on my review of records from Apple, Subject Account 1 contained several identity documents and photographs of PONLE. These included a photo of a Nigerian passport with a photo of an individual named Olalekan Jacob Ponle, born in May 1991 in Lagos, Nigeria, a photo of a United Arab Emirates visa with a photo of an individual named Olalekan Jacob Ponle with the profession “marketing

¹ Voice over Internet Protocol, or VOIP, is a technology that allows callers to use an internet connection for voice calls. As a result, the user of a VOIP application can be anywhere in the world, so long as they have an internet connection.

representative” and a photo of a United Arab Emirates Resident Identity Card with a photo of a Nigerian national named Olalekan Jacob Ponle.

17. I reviewed a January 2012 United States visa application which included a photograph and biographical data for an individual named Olalekan Jacob Ponle, born in May 1991, in Lagos, Nigeria, and the images and biographical information matched the information contained in the passport photo, the United Arab Emirates (UAE) visa and the UAE Resident Identity Card recovered from Subject Account 1. I have included these photos below:

- a. Photo from a United States visa application in the name of



PONLE:

- b. Photo from Subject Account 1 of a Nigerian passport in the name



of PONLE:

- c. Photo from Subject Account 1 of a UAE visa in the name of



PONLE:

- d. Photo from Subject Account 1 of a UAE Resident Identity Card in



the name of PONLE:

18. I have reviewed activity records for Subject Account 1 between February 16, 2020 and March 10, 2020 and observed that, according to whois² records, most of the IP addresses used to access Subject Account 1 are assigned to internet service providers located in the UAE.

19. In addition to these identity documents, Subject Account 1 included three photos and two videos of an individual who appears to be PONLE, appearing by himself and looking into the camera; a photo of a DHL shipping label with recipient details including the name Olalekan Jacob Ponle and an address located in Dubai, UAE; and a photo of a DHL shipping label with recipient details including the name Olalekan Jacob Ponle and another address located in Dubai, UAE.

² Whois is an open source tool used for querying databases that store the registered users or assignees of Internet resources such as domain name and IP address blocks.

20. Additionally, based on my review of Subject Account 1 records, I saw several WhatsApp conversations between PONLE and other individuals in which PONLE identified himself by name. For example, on or about March 6, 2019, in a conversation that appeared to discuss sending wire transfers, PONLE and an unknown individual (“Individual C”) exchanged the below messages:

PONLE: Just send 60k to the account as directed

PONLE: Use my name as Reference

PONLE: OLALEKAN JACOB PONLE

Individual C: k

21. Also, for example, on or about June 18, 2019, in a conversation that appeared to be of a social nature, PONLE and an unidentified individual (“Individual D”) exchanged the below messages:

Individual D: This is my name

Individual D: First: [Individual D first name]

Last: [Individual D last name]

Individual D: Now you know my full government

Individual D: Tell me yours

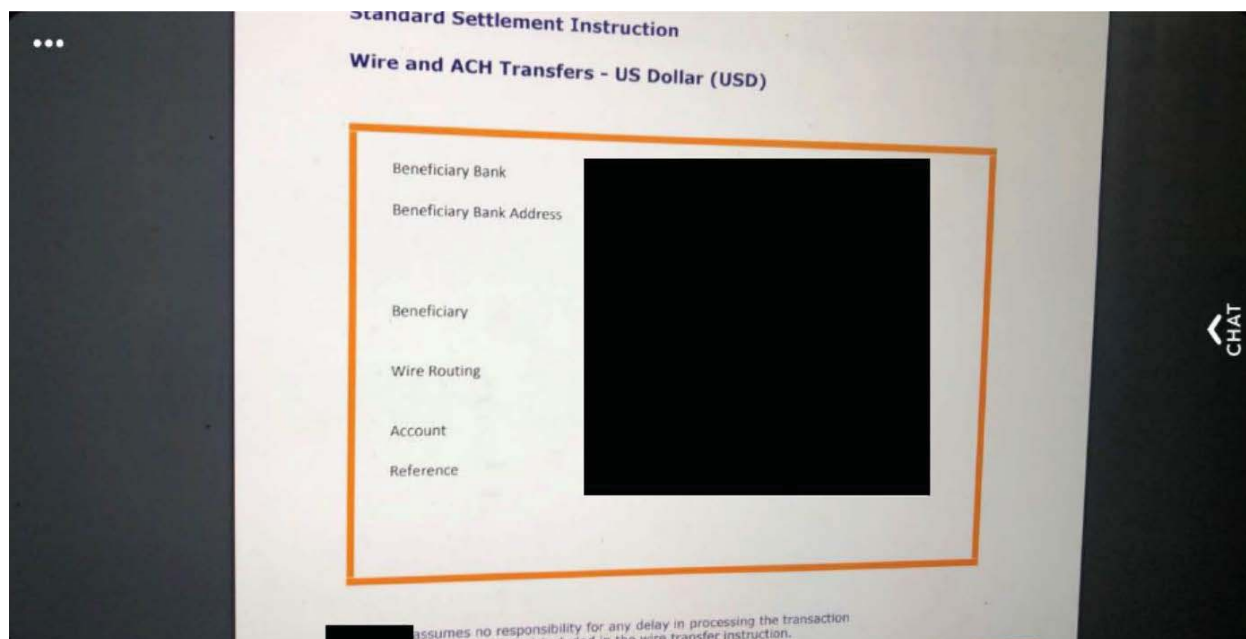
PONLE: Jacob Ponle

Individual D: Where did Woodie come from

PONLE: It came from a friend awarding me that name cause I used to be a comedian in high school

PONLE: and ever since I retained it

22. Finally, as described in more detail below, Subject Account 1 also contained WhatsApp conversations with other individuals discussing wire transfers as well as images of computer screens displaying what appear to victim company emails containing wire transfer instructions or financial information. For example, the following image was found in Subject Account 1:



23. Based on my training and experience, criminals who engage in business email compromise schemes coordinate wire transfers with co-conspirators using WhatsApp and other online messaging applications and sometimes share images of compromised victim company email accounts. Based on these observations and information I obtained from law enforcement databases and interviews with victim companies, I believe PONLE collaborated with co-conspirators to engage in business email compromise schemes.

B. PONLE Was Involved in a January 16, 2019 Business Email Compromise Scheme Targeting Victim Company B

24. On or about January 16, 2019, a business email compromise scheme targeting Victim Company B, located in Des Moines, Iowa, resulted in a fraudulent wire of approximately \$188,000 to a bank account in the name of a Victim Company B supplier. As described below, PONLE directed Individual B to open a bank account in the name of the Victim Company B supplier, told Individual B the amount of money that would be wired to the account, directed Individual B to convert the proceeds of the BEC to Bitcoin, and directed Individual B to send the proceeds to the 16AtGJ BTC Wallet.

25. Based on a review of text messages exchanged by PONLE using the 4088 telephone number and the alias “Mark Kain”³ and Individual B, PONLE first contacted Individual B about Victim Company B on January 7, 2019.

26. At approximately 9:06 PM UTC on January 7, 2019 PONLE and Individual B had the following exchange:

PONLE:	I want you to set up a separate business account just to receive the money In this name [Victim Company B supplier]
Individual B:	They will ask me what type of business
PONLE:	just a small scale business or something intriguing to tell them Then right away we kick start to process the wire for 200k.

³ For the reasons stated above, I believe that “Mark Kain” is an alias used by PONLE. When exchanging the messages with Individuals A and B described in this affidavit, PONLE used that alias. For clarity, I will refer to PONLE by his true name throughout.

Individual B: [Individual B] dba [Victim Company B supplier]
[account number ending 8208]
ABA# 061000104.

Based on the content and context of this text, I understand that Individual B had set up an account in the name of the Victim Company B supplier and provided the account and routing number to PONLE.

26. At approximately 12:27 PM UTC on January 10, 2019, PONLE texted, “The wire has been processed and I believe it should be in the account now[.] \$188k.”

27. Based on information provided by an employee of Victim Company B, on or before January 16, 2019, one or more unknown subjects gained unauthorized access to a Victim Company B-issued email account by compromising the credentials through phishing. The unknown subjects then changed security settings in the email account to hide their activity from the account user. On or about January 16, 2019, the unknown subjects used this access to send an email from the Victim Company B Email Account. The email requested a \$188,000 wire transfer from Victim Company B to the Victim Company B supplier at the 8208 bank account. As a result of the fraudulent email \$188,000 was sent to 8208 account, the same account created by Individual B at PONLE’s direction.

28. Beginning at approximately 3:13 PM UTC on or about January 17, 2019, PONLE and Individual B had the following exchange:

Individual B: The money is in
Send me your wallet.

PONLE: [The 16AtGJ Wallet]

Individual B: Just sent 121,000.

PONLE: Received.

29. Blockchain analysis and records from a cryptocurrency exchange services, confirmed that on or about January 17, 2019 Individual B sent approximately 3.13030959 bitcoin, worth approximately \$119,000 at the time of the transaction, from Individual B's account to PONLE's 16AtGJ BTC Wallet.

30. Text messages between Individual B and PONLE shortly after the January 16, 2019 BEC show PONLE's knowledge of the fraudulent nature of these financial transactions. For example, beginning at approximately 2:58 PM UTC on or about January 22, 2019, PONLE and Individual B had the following exchange:

PONLE: If I need you to set up another name account can you do that today.

Individual B: A new fictitious name?

PONLE: Yes
[Individual B] I really enjoy the relationship we are building and I'll sincerely want us to work for a long time but we most [sic] develop a very creative statistics to beat this banks in other for them not to stop our dealings.

Individual B: How do we do that.

PONLE: Having more bank account and each time we done with it we move to the next one.
that way we probably use them for 1-2 transaction at most.

Individual B: You're probably right.

C. PONLE Was Involved in a February 11, 2019 Business Email Compromise Scheme Targeting Victim Company A

31. On or about February 11, 2019, a business email compromise scheme targeting Victim Company A, located in Chicago, resulted in a fraudulent wire of approximately \$2,300,000 to a bank account in the name of a Victim Company A subsidiary opened by Individual A at PONLE's direction.

32. As described below, based on a review of text messages exchanged by PONLE and Individual B, between approximately February 8, 2019 and February 15, 2019, PONLE directed Individual B to open a bank account in the name of the Victim Company A Subsidiary and coordinated a wire transfer of \$2,300,000 into this account. PONLE further instructed Individual B as to how to disburse those funds.

33. At approximately 4:52 PM UTC, on or about February 8, 2019, PONLE and Individual B exchanged the followed messages:

PONLE: Good morning [Individual B]
[the Victim Company Subsidiary] is the new name we
should used [sic].

Individual B: Yes I'm on it but I want my [sibling] to open account But I
will control everything.

PONLE: 2.3M is the figure for this
Can you do with Bank of America?

31. Based on my review of additional correspondence and bank records, I know that on or about February 8, 2019, Individual A, who is Individual B's sibling, began working with PONLE and Individual B to open a bank account.

32. Based on an interview with the Vice President and Controller ("Employee A") at Victim Company A and Victim Company A records, at some point

on or before February 11, 2019, one or more unknown subjects gained unauthorized access to a Victim Company-issued email account (the “Victim Company A Email Account”) belonging to the Chief Accounting Officer of a subsidiary of the Victim Company (the “Victim Company A Subsidiary”).

33. On or about February 11, 2019, the unknown subjects used this access to send an email from the Victim Company A Email Account to Employee A’s email account. The email included an attachment requesting a \$2,300,000 wire transfer from the Victim Company to the Victim Company Subsidiary at Bank of America account number xxxxxxxx7046 (“the 7046 Account”). The fraudulent email was almost identical to a prior, legitimate email from the Victim Company A Email Account to Employee A’s email account. Specifically, the email and attachment included the same wire transfer amount, the name of the Victim Company Subsidiary, the same beneficiary account routing number and the same beneficiary account name. The only difference was the email’s date and the beneficiary account number.

34. Bank of America records show that Individual A opened the 7046 Account in-person on or about February 11, 2019 under Individual A’s true name “d/b/a [the Victim Company Subsidiary]”. Account opening documentation includes Individual A’s social security number and a signature. The 7046 account is a business checking account.

35. Beginning at approximately 2:03 PM UTC February 11, 2019, PONLE and Individual B had the following exchange:

Individual B: Hey [PONLE]. Do I have your approval to give your number to my [sibling] because [s/he] is setting it up and [s/he] needs to ask you a few questions?

PONLE: Okay go ahead.

Individual B: Ok [his/her] name is [Individual A].

36. At approximately 12:56 AM UTC on or about February 12, 2019, Individual B texted, "Everything is ready to go."

37. On or about February 14, 2019, personnel at the Victim Company, relying on the February 11, 2019 fraudulent wire transfer request, sent a \$2,300,000 wire transfer to the 7046 Account.

38. Beginning at approximately 6:01 PM UTC February 14, 2019, PONLE and Individual B discussed having Individual A send the proceeds of the \$2,300,000 wire transfer to PONLE:

PONLE: Hey can you check [if] the funds arrived now.

Individual B: It's in!!!
[S/he]'s doing the wire now
2.3
I'm instructing [him/her] and on it.

39. Later the same day, February 14, 2019, \$2,300,000 was sent from the 7046 Account to a second Bank of America account, number xxxxxxxx6046 ("the 6046 Account") via an online banking transfer. Bank of America records show that the 6046 Account is a personal checking account that was opened online by Individual A on or about September 24, 2018.

40. On or about February 15, 2019, a \$2,149,000 wire transfer was sent from the 6046 Account to Silvergate Bank account number xxxxxxxx8012 ("the 8012

Account”). The 8012 Account belongs to Gemini Trust, a cryptocurrency exchange business, and is used by Gemini Trust to facilitate customer transactions. The February 15, 2019 wire transfer included the beneficiary notation, ZVZPZV, and federal IMAD number, 20190215B6B7HU3R006023.

41. Records obtained from Gemini Trust show that the beneficiary notation ZVZPZV and federal IMAD number 20190215B6B7HU3R006023 are associated with Gemini Trust customer account xxxxxxxx9581 (“the 9581 Account”), which was owned by Individual A.

42. Beginning at approximately 4:48 PM UTC on or about February 15, 2019, PONLE and Individual B had the following exchange:

Individual B: The money is in the exchange
[Individual A] is going to start doing the block trading.
We are going to send you 500k at a time until you have it
all.

PONLE: Wallet is
[the 16AtGJ BTC Wallet]

Individual B: [S/he] is getting ready to send you 340 [bit]coins
Sent
And the rest is coming.

PONLE: I got the first one
I got the second one just waiting for remainder.

Individual B: Just sent the last 36k

43. Gemini Trust records showed that on February 15, 2019, the 9581 Account received a \$2,149,000 wire transfer deposit and that within approximately the next 90 minutes, approximately \$2,148,877.70 was converted from U.S. Dollars

to bitcoin and subsequently transferred in two separate transactions to the 16AtGJ BTC Wallet.

D. PONLE Was Involved in a March 4, 2019 Business Email Compromise Scheme Targeting Victim Company H

44. Based on information provided by a company located in Great Bend, Kansas ("Victim Company H") and records provided by PNC Bank, on or before March 4, 2019, one or more unknown subjects gained unauthorized access to a Victim Company H-issued email account. The unknown subjects then made rule changes to the compromised email account to prevent their activity from being detected by the account user. On or about March 1, 2019, the unknown subjects used this access to send an email from the Victim Company H Email Account to a creditor of Victim Company H requesting a \$415,000 wire transfer to a PNC Bank account in the name of Victim Company H opened by Individual B at PONLE's direction. As a result of the fraudulent email, on or about March 4, 2019, PNC bank records show that a wire transfer of approximately \$415,000 was sent from Victim Company H's creditor to the account owned by Individual B.

45. Based on a review of text messages exchanged by PONLE and Individual B between approximately February 26, 2019 and February 28, 2019,

several days before the fraudulently-induced wire transfer, PONLE directed Individual B to open a bank account in the name of the Victim Company H.

46. At approximately 4:38 PM UTC, on or about February 26, 2019, PONLE sent Individual B this message: “I have a new name I need you to work on ASAP[.] [Victim Company H]”

47. Beginning at approximately 3:02 PM UTC, on or about February 28, 2019, PONLE and Individual B exchanged the following messages:

PONLE: [Victim Company H] I’m waiting for the account this morning

Individual B: I will have the account number very shortly

48. Beginning at approximately at approximately 9:00 PM UTC on or about February 28, 2019, PONLE and Individual B exchanged the following messages:

Individual B: [account number ending 0495 (the “0495 account”)]
PNC bank

PONLE: This belongs to [Victim Company H] right

Individual B: Yes

Based on the content and context of this exchange, I believe that Individual B had opened a bank account in Victim Company H’s name, per PONLE’s earlier request.

49. Based on my review of Subject Account 1 records, I saw several WhatsApp conversations between PONLE and other individuals who appear to be involved in business email compromise schemes. Based on my training and experience, criminals typically work with co-conspirators in order to perpetrate these schemes. The criminals and their co-conspirators often share details relevant to the

schemes, such as bank account information, with one another via messaging applications such as WhatsApp.

50. Between February 22, 2019 and March 18, 2019, approximately 275 messages were exchanged between PONLE and Co-conspirator 1 (“CC-1”). Many of these messages discussed bank account details and various “jobs”, which I believe refer to business email compromise schemes. For example, at approximately 5:12 PM UTC on or about March 1, 2019, PONLE and CC-1 exchanged the below messages:

CC-1:	That job [Victim Company H]
PONLE:	Yes
CC-1:	I don update d aza
PONLE:	Okay good
CC-1:	Dem don reply Monday I go instruct dem respond Monday 400k

Based on my training and experience and open source information, the word “aza” is a slang term used by Nigerian cyber criminals to refer to a bank account, typically those used to deposit money obtained through fraud.

51. Within one minute of the text exchange with CC-1, at approximately 5:13 PM UTC on or about March 1, 2019, PONLE texted Individual B: The [Victim Company H] has 400k coming on Monday.

52. Beginning at approximately 5:20 PM UTC on or about March 4, 2019, PONLE and Individual B exchanged the following messages:

PONLE: The \$415k will arrive the PNC today just keep checking it
Individual B: We have the money. Setting up wires now

E. PONLE Was Involved in a June 2019 Business Email Compromise Scheme Targeting Victim Company M

55. Based on information obtained from an interview of personnel at Victim Company M, in or about May 2019, an administrative account in Victim Company M’s email system was compromised by unknown actors. The unknown actors created email forwarding rules that allowed them to read emails belonging to high-ranking employees at Victim Company M.

56. In or about June 2019, Victim Company M personnel received emails from an email address with a domain spoofed to appear similar to the name of the company that distributes Victim Company M’s quarterly dividends. On or about June 11, 2019, Victim Company M personnel received a fraudulent email with instructions to wire \$19,292,690.30 to a bank account ending in 6552 (“the 6552 account”). Victim Company M Personnel attempted to send the wire transfer as

instructed, but the transaction failed because the 6552 account was closed by the bank for fraud. On or about June 19, 2019, Victim Company M personnel received another fraudulent email from the same email address stating that there was a problem with the previous bank account and with instructions to wire the same amount to an account ending in 1295 (“the 1295 account”). Victim Company M Personnel attempted to send the second wire transfer as instructed, but the transaction failed because the 1295 account had also been closed for fraud.

57. Based on my training and experience, criminals and their co-conspirators involved in business email compromise schemes gain unauthorized access to victim company email accounts, look for emails pertaining to wire transfers and then share images of these emails with co-conspirators in order to coordinate the creation of bank accounts to receive a fraudulently-induced wire transfers. Additionally, these criminals sometimes share images of details of bank accounts created by mules to launder the funds from these schemes. I reviewed the contents of Subject Account 1 and observed approximately five images that show that PONLE had access to emails and financial records for Victim Company M. Based on the overlapping information in these images and the information provided by Victim Company M, I believe that PONLE and other co-conspirators were involved the scheme targeting Victim Company M. The images included:

a. A photo of a computer screen displaying an email with the following text:

Please approve the attached Dividend payment (including postage) of **\$19,292,690.30** set for **June 20th**. I have reviewed the funding letter from

[Transfer Services Company] for accuracy and validated the share count included in the payment amount. Even though the attached Daily Transaction Journal file is dated 5/31/2019, according to [Transfer Services Company], there has been no change in the number of outstanding shares since then.

Dividend Payment Reconciliation **Jun-19**

Total # of shares: 385,837,581
Dividend / Share: \$0.050
Dividend Payment Amount: \$19,291,879.05
Postage: \$811.25
Total Dividend Payment Amount: \$19,292,690.30

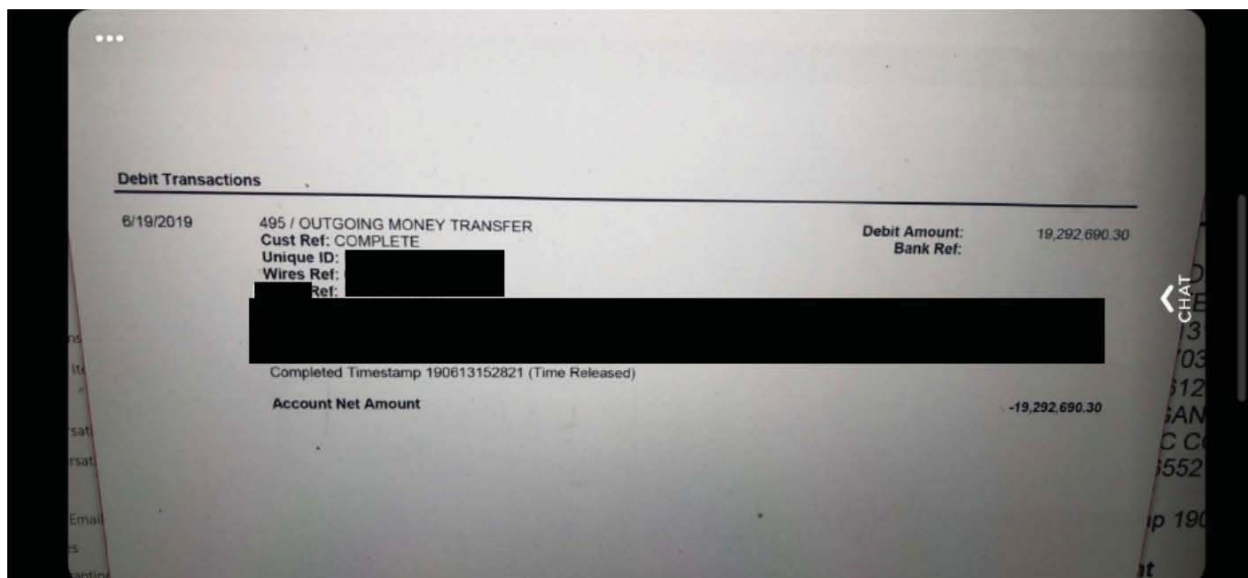
Corporate Treasury - Please note the bank name & associated ABA number in the funding request:

Bank Name: JP Morgan Chase
ABA Number: 121000021
A/C Name: [Transfer Services Company] as agent for [Victim Company M]
A/C Number: XXX-XX6552 ("the 6552 account")

Please let me know if you have any questions.

The "Total Dividend Payment Amount" contained in the screenshot of the Victim Company M email is the same amount requested in the June 11, 2019 and June 19, 2019 fraudulent emails.

b. A photo of a computer screen displaying what appears to a debit transaction record dated June 19, 2019 for an outgoing money transfer from Victim Company M in the amount of \$19,292,690.30:



c. An image of what appeared to be a photo of a computer screen displaying a web page with bank account details identifying Victim Company M, the 1295 account, and the Transfer Services Company. The screenshot listed the available balance in the account. Based on my training and experience, I believe this screenshot was taken and sent to PONLE to inform him that the 1295 account was open and available for use.

F. PONLE Was Involved in a September 6, 2019 Business Email Compromise Scheme Targeting Victim Company I

59. Beginning on or about July 12, 2019, an FBI online covert employee (“OCE-1”) began communicating with PONLE using a messaging application handle that was previously used by Individual A. Subsequently, PONLE directed OCE-1 to open two bank accounts in the names of companies in the United States in order to receive wire transfers and to transfer any funds sent to those accounts to the 16AtGJ BTC Wallet.

60. More specifically, on or about July 15, 2019, via an online messaging application, PONLE directed OCE-1 to open a bank account in the name of Company B. In response, the FBI opened the Covert Company B bank account. On or about July 17, 2019, OCE-1 provided PONLE the Covert Company B bank account information.

61. While no money was ever sent to the Covert Company B bank account, based on information provided by personnel at a company located in Southfield, Michigan ("Victim Company I"), I learned that on or before September 6, 2019, unknown subjects gained unauthorized access to two Victim Company I email accounts belonging to its two co-owners. The unknown subjects used that access to send emails to Victim Company I personnel from both compromised email accounts requesting a wire transfer of \$1,206,418.76 and identifying the receiving account number as the Covert Company B bank account opened at PONLE's instruction in July 2019. Personnel at Victim Company I determined that the wire transfer request was fraudulent, and no funds were sent.

G. PONLE Was Involved in a September 9, 2019 Business Email Compromise Scheme Targeting Victim Company J

62. Based on interviews with personnel at a company located in Harrison, New York ("Company D"), Company D and Victim Company J, located in Garden City, New York were involved in a real estate transaction in 2019. In connection with this transaction, several days prior to September 9, 2019, Company D sent Victim Company J an email containing a loan payoff letter and wire transfer instructions.

63. On or about September 9, 2019, unknown subjects sent Victim Company J personnel a fraudulent email from a spoofed email address. Based on my training and experience, spoofed email addresses are designed to look like a real domain in order to trick a recipient into responding. Email spoofing is commonly used in BEC schemes.

64. The fraudulent email contained a loan payoff letter with wire transfer instructions identifying the receiving account number as the Covert Company B bank account opened at PONLE's instruction in July 2019, and the same account used in the attempt to defraud Victim Company I. Personnel at Victim Company J determined that the wire transfer request was fraudulent, and no funds were sent.

H. PONLE Was Involved in a September 4 through September 9, 2019 Business Email Compromise Scheme Targeting Victim Companies K and L

65. Based on interviews with personnel at a company located in Chicago, Illinois ("Victim Company K") and a company located in Santa Ana, California ("Victim Company L"), in or about February 2019, unknown subjects set up an escrow with Victim Company L with account holder information that Victim Company L later determined to be fictitious.

66. On or about July 23, 2019, via an online messaging application, PONLE directed OCE-1 to open a bank account in the name of Company C. In response, the FBI opened the Covert Company C bank account. On or about July 17, 2019, OCE-1 provided PONLE the Covert Company C bank account information.

67. On or before September 4, 2019, unknown subjects gained unauthorized access to a Victim Company K email account. On September 4, 2019, the unknown actors used that access to send emails to Victim Company K personnel to induce a wire transfer of \$5,000,000 to the escrow account at Victim Company L that was set up in February 2019. On the same date, unknown actors sent a separate email inducing Victim Company K to wire \$268,000 to a fraudulent account.

68. After the escrow account was credited \$5,000,000, the unknown subjects then communicated via email and phone with personnel at Victim Company L to attempt to induce a wire transfer of approximately \$4,000,000 of the funds to Covert Company C bank account, which was opened at PONLE's direction in July 2019, and the remaining \$1,000,000 to two other bank accounts. Personnel at Victim Company L determined that the wire transfer requests were fraudulent, and no funds were sent.

69. The online communications between OCE-1 and PONLE show that PONLE had specific knowledge of details about the business email compromise schemes targeting Victim Companies K and L. For example, PONLE and OCE-1 exchanged the following online messages on or about September 4, 2019:

PONLE:	The [to Covert Company C bank account] account would be funded today
OCE-1:	Funded as in today or tomorrow?
PONLE:	Yes the transaction is being processed as we speak just wanted you to be on alert
PONLE:	It's coming from California

70. Separately, based on an interview of personnel at Victim Company K, on or about September 9, 2019, unknown subjects gained unauthorized access to a Victim Company K email account and used the account to send emails to Victim Company K personnel to induce two wire transfers of \$5,000,000. They identified Covert Company C bank account as the recipient bank account for one of the transfers. On or about September 9, 2019, personnel at Victim Company K sent the funds to Covert Company C bank account.

71. PONLE's messages to OCE-1 on September 9, 2019, demonstrate his knowledge of this BEC scheme:

PONLE: [OCE-1], great news I have the funds have being wired into [Covert Company C bank account] I have the confirmation right now as we speak.

OCE-1: Wonderful!!! The funds are in there [PONLE]! I'm glad they finally came through
Transferring to my personal account as we speak

PONLE: Excellent

OCE-1: Everything should move over in the next 24-48 hours

PONLE: All coins would be ready ?

OCE-1: Yup, moving over to the exchange. Might take up to 48 hours
What is your wallet address?

PONLE: Same one I being using
[the 16AtGJ BTC Wallet]

III. CONCLUSION

72. Based on the above information, there is probable cause to believe that, beginning no late than January 2019 and continuing until at least September 2019,

at Chicago, in the Northern District of Illinois, Eastern Division, and elsewhere,
PONLE conspired to commit wire fraud, in violation of 18 U.S.C. § 1349.

FURTHER AFFIANT SAYETH NOT.

SADIQ.ALI.G95F98E79

2020.06.25 16:48:19 -05'00'

ALI SADIQ

Special Agent, Federal Bureau of
Investigation

SUBSCRIBED AND SWORN to before me on June 25, 2020.

 _____

United States Magistrate Judge